

The diagram illustrates a secure mail system architecture with the following components and data flow:

- USPS Certificate Authority (10)**: Issues certificates and public keys.
- Operations Center (12)**: Receives the **Certificate/Public Key & Certificate ID** from the USPS Certificate Authority.
- PGD (14)**: Receives data from the Operations Center (via a monitor 16 and keyboard 18) and outputs a **Digital Signature & Certificate ID** (22).
- USPS Distribution Center (Verifier) (20a)**: Receives the **Certificate ID** from the PGD and sends a **Valid** response to the **USPS Distribution Center (Destination) (20b)**.
- USPS Certificate Authority (10)**: Also sends a **Certificate/Public Key** directly to the **USPS Distribution Center (Verifier) (20a)**.

Labels for the distribution centers are **Destination** (20b) and **Origin** (20a).

FIG. 1

0960357 080300

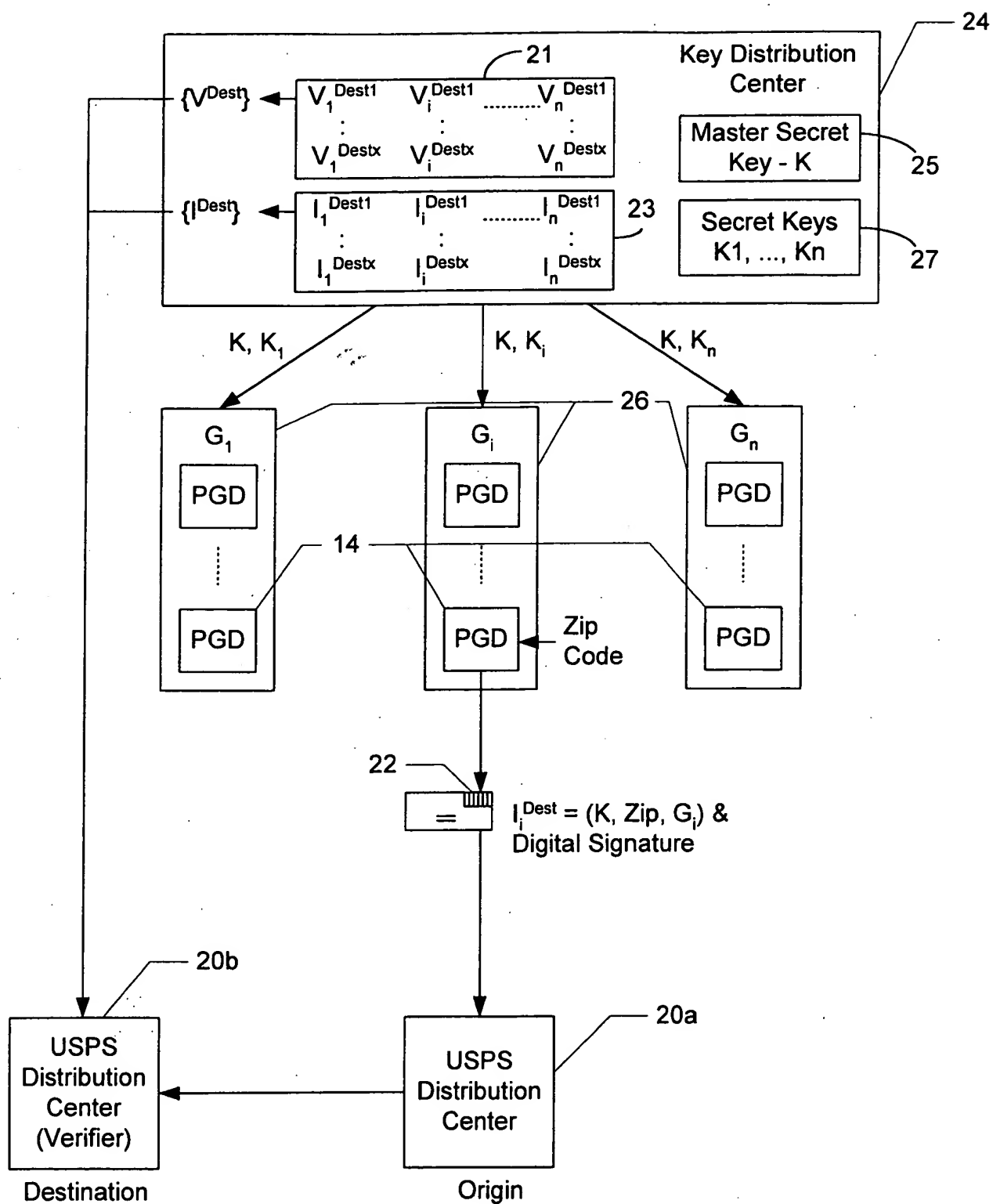


FIG. 2

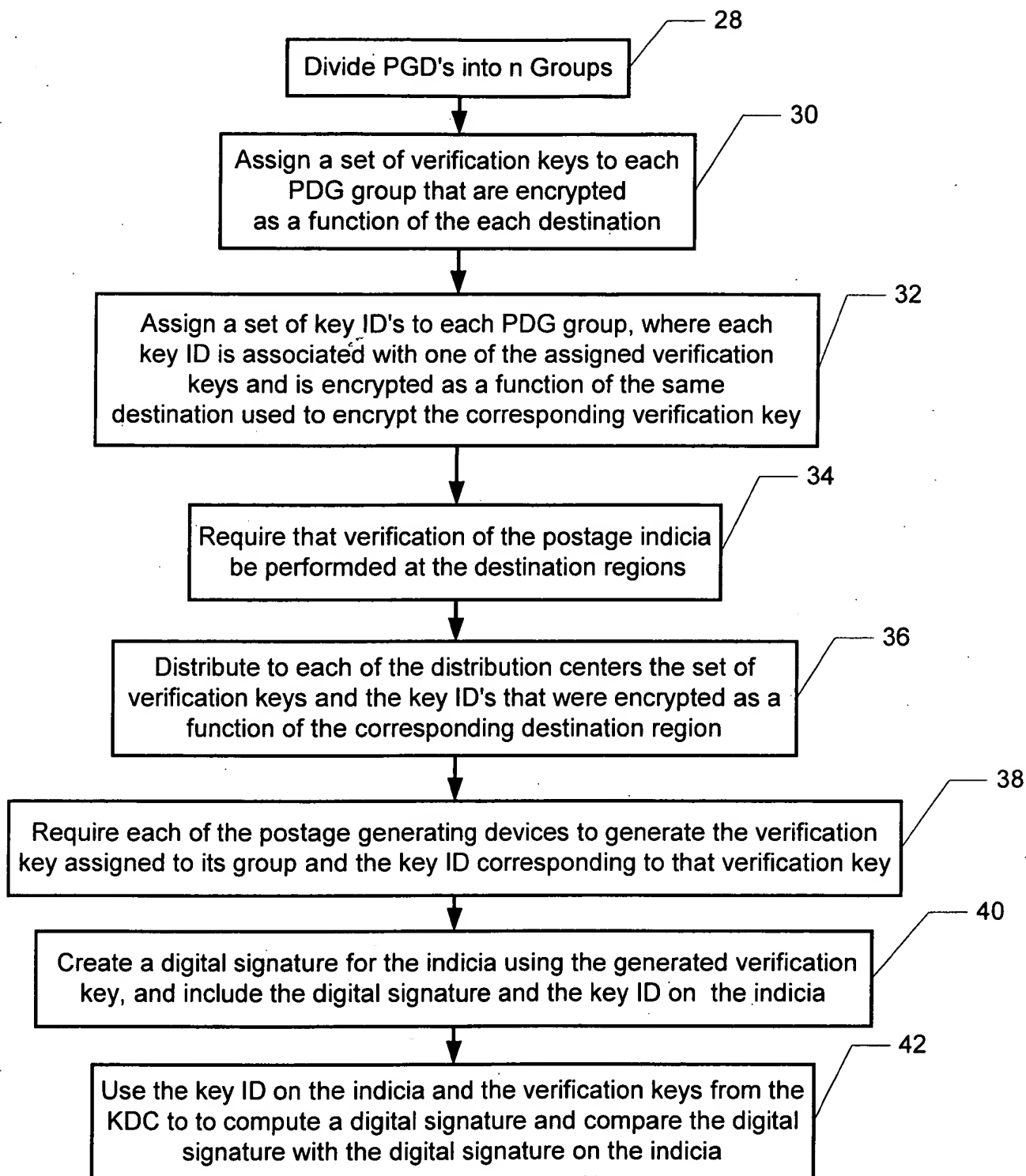
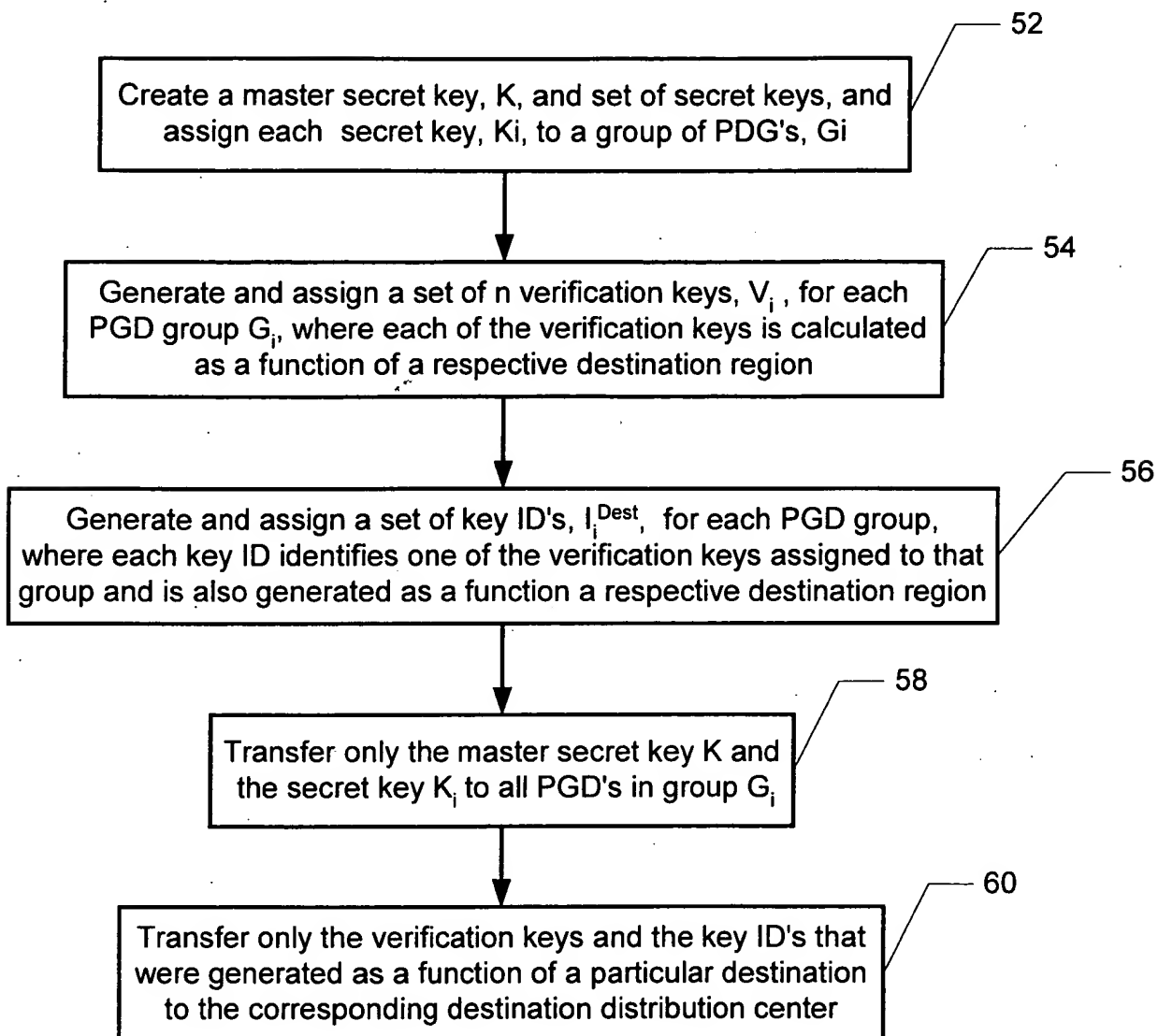


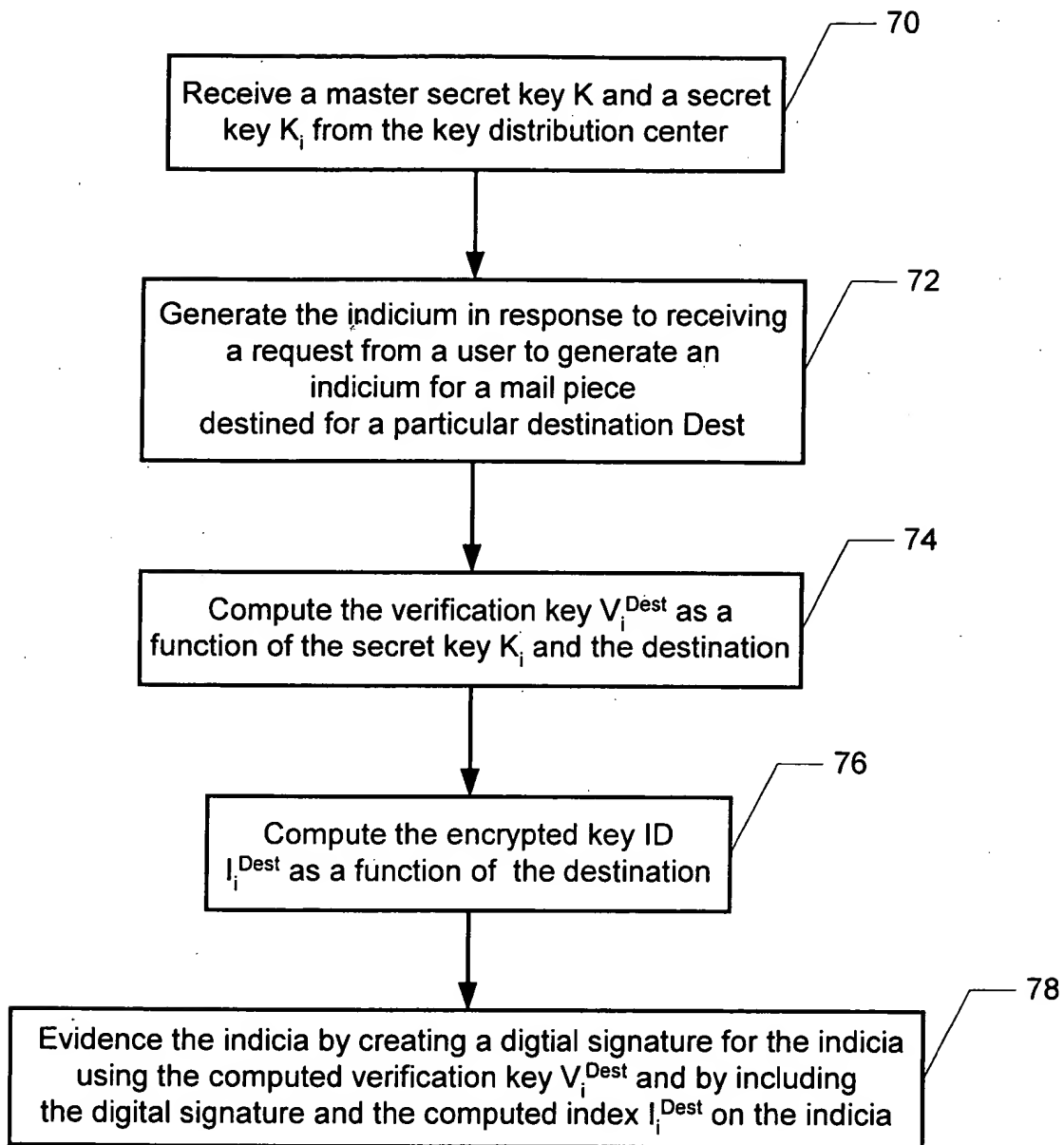
FIG. 3



Generation and Distribution of Keys

FIG. 4

036874-24



Dispensing & Evidencing Postage Indicia

FIG. 5

```
graph TD; 90[Receive the verification keys V_i^Dest and key ID's I_i^Dest generated as a function of the destination region serviced by the distribution center] --> 92[In response to receiving a mail piece, determine the mail piece's destination region]; 92 --> 94[If the distribution center is not within the destination region, transfer the mail piece to the distribution center within the destination region]; 94 --> 96[If the distribution center is within the destination region, begin verifying the postage indicia by reading the digital signature and the key ID from the indicia]; 96 --> 98[Use the key ID read from the indicia to retrieve the corresponding verification key from the table of all verification keys]; 98 --> 100[Use the retrieved verification key to compute a digital signature for the indicia, and compare the computed digital signature with the digital signature from the postage indicia to verify the indicia];
```

900

90 Receive the verification keys V_i^{Dest} and key ID's I_i^{Dest} generated as a function of the destination region serviced by the distribution center

92 In response to receiving a mail piece, determine the mail piece's destination region

94 If the distribution center is not within the destination region, transfer the mail piece to the distribution center within the destination region

96 If the distribution center is within the destination region, begin verifying the postage indicia by reading the digital signature and the key ID from the indicia

98 Use the key ID read from the indicia to retrieve the corresponding verification key from the table of all verification keys

100 Use the retrieved verification key to compute a digital signature for the indicia, and compare the computed digital signature with the digital signature from the postage indicia to verify the indicia

FIG. 6